Boletín de Ciberseguridad N°69

Fecha de publicación: 23/10/2023

Mes de Octubre

09/10/2023 – 23/10/2023

Datasec

BOLETÍN DE CIBERSEGURIDAD

Indice

Introducción

Por medio de este boletín informativo estaremos destacando de forma quincenal, las noticias más relevantes en el ámbito de la ciberseguridad a nivel regional e internacional.

Las principales categorías de información son: vulnerabilidades tecnológicas, fraudes activos, amenazas por medios informáticos nuevos, así como recomendaciones específicas de prevención. La publicación de dichas noticias dependerá de la importancia y calidad informativa de las mismas.

A su vez se incluyen referencias técnicas y de gestión a los efectos de reducir los riesgos con anticipación y adecuada planificación.

En esta segunda quincena del mes de octubre se destacan 5 noticias de relevancia: 2 sobre vulnerabilidades tecnológicas, y 3 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Vulnerabilidad de día cero de Cisco

Cisco advirtió sobre una falla de seguridad crítica y sin parches que afecta al software IOS XE y que está bajo explotación activa en la naturaleza.

CISA advierte sobre vulnerabilidad de Adobe Acrobat Reader

CISA agregó el martes una falla de alta gravedad en Adobe Acrobat Reader a su catálogo de vulnerabilidades explotadas conocidas (KEV), citando evidencia de explotación activa.

Microsoft lanza parches de octubre de 2023 para 103 fallas

Microsoft lanzó sus actualizaciones del martes de parches para octubre de 2023, abordando un total de 103 fallas en su software, dos de las cuales han sido explotadas activamente en la naturaleza.

Vulnerabilidad Crítica

CISCO	Vulnerabilidad de día cero de Cisco	CRÍTICO

Descripción

Cisco advirtió sobre una falla de seguridad crítica y sin parches que afecta al software IOS XE y que está bajo explotación activa en la naturaleza.

Estado

Arraigada en la función de interfaz de usuario web, la vulnerabilidad de día cero se rastrea como CVE-2023-20198 y se le ha asignado la calificación de gravedad máxima de 10,0 en el sistema de puntuación CVSS.

Vale la pena señalar que la deficiencia solo afecta a los equipos de redes empresariales que tienen habilitada la función de interfaz de usuario web y cuando están expuestos a Internet o a redes que no son de confianza.

El problema afecta tanto a los dispositivos físicos como a los virtuales que ejecutan el software Cisco IOS XE y que también tienen habilitada la función de servidor HTTP o HTTPS. Como mitigación, se recomienda desactivar la función del servidor HTTP en los sistemas conectados a Internet.

Remediación / Referencias

Cisco proporcionará una actualización sobre el estado de nuestra investigación a través del aviso de seguridad. Consulte el aviso de seguridad y el blog de Talos para obtener detalles adicionales.

Por más información acceder a:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

	CISA advierte sobre vulnerabilidad de Adobe Acrobat Reader	CRÍTICO

Descripción

CISA agregó el martes una falla de alta gravedad en Adobe Acrobat Reader a su catálogo de vulnerabilidades explotadas conocidas (KEV), citando evidencia de explotación activa.

Estado

Registrada como CVE-2023-21608 (puntuación CVSS: 7,8), la vulnerabilidad se ha descrito como un error de uso después de la liberación que puede explotarse para lograr la ejecución remota de código (RCE) con los privilegios del usuario actual.

Adobe lanzó un parche para la falla en enero de 2023. A los investigadores de seguridad de HackSys, Ashfaq Ansari y Krishnakant Patil, se les atribuyó el mérito de descubrir e informar la falla.

Las siguientes versiones del software se ven afectadas:

- Acrobat DC: 22.003.20282 (Win), 22.003.20281 (Mac) y versiones anteriores (corregidas en 22.003.20310)
- Acrobat Reader DC: 22.003.20282 (Win), 22.003.20281 (Mac) y versiones anteriores (corregidas en 22.003.20310)
- Acrobat 2020 - 20.005.30418 y versiones anteriores (corregido en 20.005.30436)
- Acrobat Reader 2020 - 20.005.30418 y versiones anteriores (corregido en 20.005.30436)

Actualmente se desconocen los detalles sobre la naturaleza de la explotación y los actores de amenazas que pueden estar abusando de CVE-2023-21608. A finales de enero de 2023 se puso a disposición un exploit de prueba de concepto (PoC) para la falla.

Remediación / Referencias

Se deben aplicar los parches proporcionados por los proveedores antes del 31 de octubre de 2023 para proteger sus redes contra posibles amenazas.

Por mayor información acceder a:

https://nvd.nist.gov/vuln/detail/CVE-2023-21608

Prevención

Microsoft	Microsoft lanza parches de octubre de 2023 para 103 fallas	PREVENCIÓN

Descripción

Microsoft lanzó sus actualizaciones del martes de parches para octubre de 2023, abordando un total de 103 fallas en su software, dos de las cuales han sido explotadas activamente en la naturaleza.

Estado

De los 103 defectos, 13 están clasificados como Críticos y 90 como Importantes en cuanto a su gravedad. Esto se suma a las 18 vulnerabilidades de seguridad abordadas en su navegador Edge basado en Chromium desde el segundo martes de septiembre.

Las dos vulnerabilidades que se han convertido en armas de día cero son las siguientes:

- CVE-2023-36563 (puntuación CVSS: 6,5): una vulnerabilidad de divulgación de información en Microsoft WordPad que podría provocar la filtración de hashes NTLM
- CVE-2023-41763 (puntuación CVSS: 5,3): una vulnerabilidad de escalada de privilegios en Skype Empresarial que podría provocar la exposición de información confidencial como direcciones IP o números de puerto (o ambos), permitiendo a los actores de amenazas obtener acceso a redes internas.

La actualización de seguridad resuelve además un error grave de escalada de privilegios en Windows IIS Server (CVE-2023-36434, puntuación CVSS: 9,8) que podría permitir a un atacante hacerse pasar por otro usuario e iniciar sesión como otro mediante un ataque de fuerza bruta.

Remediación / Referencias

Microsoft ha anunciado que Visual Basic Script, que a menudo se explota para la distribución de malware, está en desuso y agregó que, en futuras versiones de Windows, VBScript estará disponible como una característica bajo demanda antes de su eliminación del sistema operativo.

Para saber más:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36563

curl://	Se descubren dos fallas de seguridad de alto riesgo en la biblioteca Curl	PREVENCIÓN

Descripción

Se han publicado parches para dos fallos de seguridad que afectan a la biblioteca de transferencia de datos Curl, el más grave de los cuales podría provocar la ejecución de código.

Estado

La lista de vulnerabilidades es la siguiente:

- CVE-2023-38545 (puntuación CVSS: 7,5): vulnerabilidad de desbordamiento de búfer basada en montón SOCKS5
- CVE-2023-38546 (puntuación CVSS: 5,0): inyección de cookies sin ningún archivo

CVE-2023-38545 es el más grave de los dos y ha sido descrito por el desarrollador principal del proyecto, Daniel Stenberg, como "probablemente el peor fallo de seguridad de Curl eLa segunda vulnerabilidad, que afecta a las versiones 7.9.1 a 8.3.0 de libcurl, permite a un mal actor insertar cookies a voluntad en un programa en ejecución utilizando libcurl en circunstancias específicas.n mucho tiempo". Afecta a las versiones de libcurl 7.69.0 hasta 8.3.0 inclusive.

Remediación / Referencias

Los parches para ambas fallas están disponibles en la versión 8.4.0 lanzada el 11 de octubre de 2023. Específicamente, la actualización garantiza que Curl ya no cambie al modo de resolución local si un nombre de host es demasiado largo, mitigando así el riesgo de desbordamientos del búfer basado en el montón.

Por más información acceder a:

https://nvd.nist.gov/vuln/detail/CVE-2023-38545

Microsoft	Microsoft eliminará NTLM en favor de Kerberos para una autenticación más sólida	PREVENCIÓN

Descripción

Microsoft ha anunciado que planea eliminar NT LAN Manager (NTLM) en Windows 11 en el futuro, ya que recurre a métodos alternativos de autenticación y refuerzo de la seguridad.

Estado

IAKerb permite a los clientes autenticarse con Kerberos en una amplia gama de topologías de red. La segunda característica, un Centro de distribución de claves (KDC) local para Kerberos, extiende el soporte de Kerberos a las cuentas locales.

Introducido por primera vez en la década de 1990, NTLM es un conjunto de protocolos de seguridad destinados a proporcionar autenticación, integridad y confidencialidad a los usuarios. Es una herramienta de inicio de sesión único (SSO) que se basa en un protocolo de desafío-respuesta que demuestra a un servidor o controlador de dominio que un usuario conoce la contraseña asociada con una cuenta.

Otra distinción crucial es que, mientras NTLM se basa en el hash de contraseñas, Kerberos aprovecha el cifrado.

Además de las debilidades de seguridad inherentes de NTLM, la tecnología se ha vuelto vulnerable a ataques de retransmisión, lo que potencialmente permite a los malos actores interceptar intentos de autenticación y obtener acceso no autorizado a los recursos de la red.

Remediación / Referencias

Todos estos cambios estarán habilitados de forma predeterminada y no requerirán configuración para la mayoría de los escenarios. NTLM seguirá estando disponible como alternativa para mantener la compatibilidad existente.

Toda la información aquí:

https://learn.microsoft.com/es-es/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-ntlm-authentication-in-this-domain

Conclusiones

En un entorno de trabajo remoto en constante evolución, la seguridad de las conexiones sigue siendo una prioridad fundamental.
Mantenernos a salvo de posibles amenazas es crucial. La actualización constante y la configuración segura de estos componentes son esenciales para mitigar riesgos. Además, es valioso contar con herramientas que evalúen la salud de los dispositivos remotos, asegurando que los sistemas operativos estén al día y los controles de seguridad estén activos.

Estas medidas no solo previenen posibles abusos o compromisos, sino que también fortalecen la ciberseguridad en general.
La implementación de soluciones como Fortinet's FortiClient Health Check o Duo Security Device Health, entre otras, puede marcar la diferencia en la postura de seguridad de una organización.

La autenticación de doble factor es un pilar en la protección de accesos remotos, reduciendo significativamente la probabilidad de incidentes de seguridad.

En Datasec, seguimos dedicados a salvaguardar la seguridad de nuestros clientes, socios y colaboradores, y alentamos a todos a mantener un enfoque constante en la seguridad cibernética.

En resumen, la seguridad en las conexiones remotas es un compromiso continuo. Al mantenerse actualizados y aplicar configuraciones seguras, las organizaciones pueden protegerse contra amenazas y garantizar un entorno de trabajo remoto seguro y confiable.

¡Sigamos trabajando juntos para mantenernos protegidos!